



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/722,655	11/28/2000	Dennis Wayne Hurst	8886.001.00	2000
25461	7590	07/29/2005	EXAMINER	
SMITH, GAMBRELL & RUSSELL, LLP			SMITHERS, MATTHEW	
1230 PEACHTREE STREET, N.E.				
SUITE 3100, PROMENADE II			ART UNIT	PAPER NUMBER
ATLANTA, GA 30309-3592			2137	

DATE MAILED: 07/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/722,655	HURST ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 18 April 2005.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 6-71 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) 19-30 and 52-62 is/are allowed.
- 6) Claim(s) 6-8,15,18,31-33,42-44,48,51,63, 64, 70 and 71 is/are rejected.
- 7) Claim(s) 9-14,16,17,34-41,45-47,49,50 and 65-69 is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date June 28, 2004
- 4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_

## DETAILED ACTION

### ***Information Disclosure Statement***

The information disclosure statement (IDS) submitted on June 28, 2004 was filed after the mailing date of the first non-final action on April 19, 2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

### ***Specification***

The disclosure is objected to because of the following informalities: On page 17, line 5, it appears the word "bit" is a typographical error.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 31-33 and 63-64 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 6,185,689 granted to Todd, Sr. et al.

Regarding claim 31, Todd meets the claimed limitations as follows:

"A process of detecting security vulnerabilities present in a target Web site, comprising:  
establishing an Internet connection with the target Web site;" see column 5, line 66 to column 6, line 14.

"retrieving a default Web page for the target Web site;  
parsing through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page;" see column 6, lines 15-25.

"scanning the target Web site for at least one known exploit in order to identify security vulnerabilities;

applying at least one predetermined hack method to the target Web site in order to identify security vulnerabilities, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory; and outputting the security vulnerabilities." see column 6, lines 40-66; column 7, lines 32-46 (The user can select a denial of service assessment . . . the user is offered a list of attacks to select . . . the BONK, BOINK, Tear Drop, LAND . . . and additional attacks can be added to the list . . .); column 8, lines 19-27 (In addition to scanning for the presence of services on the target host . . . the availability of target host files to remote viewing can be checked. . . ) and figure 6.

Regarding claim 32, Todd meets the claimed limitations as follows:

"The method of claim 31, further comprising scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities." see column 6, lines 40-66; column 7, lines 32-46 (The user can select a

denial of service assessment . . . the user is offered a list of attacks to select . . .the BONK, BOINK, Tear Drop, LAND . . . and additional attacks can be added to the list . . .); and figure 6

Regarding claim 33, Todd meets the claimed limitations as follows:  
"The method of claim 31, further comprising parsing through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages." see Todd; column 6, lines 15-25.

Claims 63 and 64 are system claims that are substantially equivalent method claims 31 and 33. Therefore claims 63 and 64 are rejected by a similar rationale.

#### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6-8, 15, 18, 42-44, 48, 51, 70 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,185,689 granted to Todd et al. and further in view of U.S. patent application 2002/0023059 granted to Bari et al.

Regarding claim 6, Todd, Sr. meets the claimed limitations as follows:  
"A process of detecting security vulnerabilities present in a target Web site, comprising:

establishing an Internet connection with the target Web site;" see column 5, line 66 to column 6, line 14.

"retrieving a default Web page for the target Web site;  
parsing through the default Web page to identify any linked-to Web pages or  
objects which are included in the default Web page;" see column 6, lines 15-25.

"scanning the target Web site for at least one known exploit in order to identify  
security vulnerabilities;

applying at least one predetermined hack method to the target Web site in  
order to identify security vulnerabilities; and outputting the security vulnerabilities." see  
column 6, lines 40-66; column 7, lines 32-46 (The user can select a denial of service  
assessment . . . the user is offered a list of attacks to select . . .the BONK, BOINK, Tear  
Drop, LAND . . . and additional attacks can be added to the list . . .); and figure 6. Todd  
further teaches a user must be authorized to perform a security assessment on the  
computer (see column 7, lines 13-28). However, Todd fails to specifically teach  
automatically passing an authorized username and password to the target Web site, if  
the username and password are required to gain access to the target Web site. Bari  
discloses a secure method for automatically logging in a user to a web site using both  
the password and username of the user (see Abstract; page 1, paragraph 0010; page 5,  
paragraph 0046; page 6, paragraph 0054 (. . . automatically logging the users onto the  
Web site with . . . user name, password . . .)). It would have been obvious to one of  
ordinary skill in the art at the time of the invention to incorporate Bari's teachings of  
securely registering and linking a user to a Web site over a network with Todd's system

for performing a security assessment using a networked website because this eliminates the user's need to remember the username and password for accessing the specific web site [see Bari; page 1, paragraph 0006].

Regarding claim 7, Todd as modified further discloses scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities." see Todd; column 6, lines 40-66; column 7, lines 32-46 (The user can select a denial of service assessment . . . the user is offered a list of attacks to select . . .the BONK, BOINK, Tear Drop, LAND . . . and additional attacks can be added to the list . . .); and figure 6

Regarding claim 8, Todd as modified further discloses parsing through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages." see Todd; column 6, lines 15-25.

Regarding claim 15, Todd as modified further discloses applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory." see Todd; column 8, lines 19-27 (In addition to scanning for the presence of services on the target host . . . the availability of target host files to remote viewing can be checked. . . ) and figure 6.

Regarding claim 18, Todd as modified further discloses applying at least one predetermined hack method includes automatically passing multiple usernames and passwords to the target Web site if a login Web page is encountered." see Bari; Abstract; page 1, paragraph 0010; page 5, paragraph 0046; page 6, paragraph 0054 ( . . . automatically logging the users onto the Web site with . . . user name, password . . . ))

Claim 42 is a system claim that is substantially equivalent method claim 6. Therefore claim 42 is rejected by a similar rationale.

Regarding claim 43, Todd as modified further discloses parsing through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages." see Todd; column 6, lines 15-25.

Regarding claim 44, Todd as modified further discloses scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities." see Todd; column 6, lines 40-66; column 7, lines 32-46 (The user can select a denial of service assessment . . . the user is offered a list of attacks to select . . . the BONK, BOINK, Tear Drop, LAND . . . and additional attacks can be added to the list . . .); and figure 6

Claim 48 is a system claim that is substantially equivalent method claim 15. Therefore claim 48 is rejected by a similar rationale.

Regarding claim 51, Todd as modified further discloses applying at least one predetermined hack method includes automatically passing multiple usernames and passwords to the target Web site if a login Web page is encountered." see Bari; Abstract; page 1, paragraph 0010; page 5, paragraph 0046; page 6, paragraph 0054 (. . . automatically logging the users onto the Web site with . . . user name, password . . . ))

Regarding claim 70, Todd, Sr. discloses everything claimed as applied above (see claim 64), and further teaches a user must be authorized to perform a security assessment on the computer (see column 7, lines 13-28). However, Todd fails to specifically teach automatically passing an authorized username and password to the target Web site, if the username and password are required to gain access to the target Web site. Bari discloses a secure method for automatically logging in a user to a web site using both the password and username of the user (see Abstract; page 1, paragraph 0010; page 5, paragraph 0046; page 6, paragraph 0054 (. . . automatically logging the users onto the Web site with . . . user name, password . . . )). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bari's teachings of securely registering and linking a user to a Web site over a network with Todd's system for performing a security assessment using a networked website because this eliminates the user's need to remember the username and password for accessing the specific web site [see Bari; page 1, paragraph 0006].

Regarding claim 71, Todd as modified further discloses scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities." see Todd; column 6, lines 40-66; column 7, lines 32-46 (The user can select a denial of service assessment . . . the user is offered a list of attacks to select . . .the BONK, BOINK, Tear Drop, LAND . . . and additional attacks can be added to the list . . .); and figure 6

***Allowable Subject Matter***

Claims 19-30 and 52-62 are allowed.

The following is an examiner's statement of reasons for allowance:

The present invention is directed towards a method and system for analyzing security flaws in a computer. Independent claims 19 and 52 recite the uniquely distinct feature of "parsing each Web page by performing a keyword search to detect points of interest identified in the linked-to Web pages or objects which are included in the default Web page. The prior art, Todd (US 6,185,689) and Bari (US 2002/0023059), discloses a conventional method and system for testing for security vulnerabilities in a computer fails to anticipate or render obvious the above underlined limitation.

Claims 9-14, 16-17, 34-41, 45-47, 49-50, and 65-69 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew B Smithers  
Primary Examiner  
Art Unit 2137